Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Commission Seeks Comment on Certain	)	GN Docket No. 12-52
Wireless Service Interruptions	)	
	)	

To: The Commission

COMMENTS OF THE
ALARM INDUSTRY COMMUNICATIONS COMMITTEE

John A. Prendergast
Salvatore Taillefer, Jr.

Blooston, Mordkofsky, Dickens,
Duffy, & Prendergast, LLP
2120 L Street NW, Suite 300
Washington, DC 20037
Tel: 202-659-0830
Fax: 202-828-5568

Filed: April 30, 2012

Table of Contents

Summary

The Alarm Industry Communications Committee ("AICC") hereby submits the following comments on several questions posed by the Commission regarding wireless service interruptions. Generally, the aggregate harm of interrupting wireless service will almost always outweigh any potential benefit. The alarm industry heavily relies upon cellular devices to transmit alarm signals of all types, and citizens increasingly report emergencies to 911 via wireless service. Silencing such transmissions, even for a limited time, would be extremely hazardous. At the same time, there is little evidence to show that disrupting service is effective; indeed, in some instances, it could make matters worse. Often, prison guards and other public safety officials use wireless phones to communicate. Moreover, numerous private sector entities provide important services that save lives, thereby enhancing public safety while reducing the burden on state and local government entities.

As technology progress, the risks associated with wireless interruptions are bound to increase. The alarm industry increasingly relies upon cellular networks as the sole communications path to the central station, and, as seen in the roll-out of NG911, wireless services such as text and multimedia messaging are increasingly used when contacting 911. On the other hand, it is likely that wireless service interruptions will become less and less effective each time one is used. While it may prevent a terrorist or criminal act the first time, the would-be perpetrators will quickly learn to accomplish their attacks in other ways, such as use of unlicensed wireless devices.

Further, a wireless interruption may accomplish the goal of one agency, while at the same time confounding the efforts of several other agencies. Once one government agency is permitted to effect a wireless service interruption, there is a high risk of creating a 'slippery slope' whereby it will be hard to tell other government agencies that they cannot use the same

measure. In light of these facts, wireless service interruptions should not be permitted without some proof of the necessity of such action. Any service interruption decision should be made by Federal officials with access to specific threat information from reliable Federal intelligence resources. While these officials could assess locally-developed intelligence and work with state and local officials as appropriate, the decision to actually interrupt service should be made at the highest level of the Federal intelligence community. Most importantly, to the extent that any situation can be found to justify a service interruption, minimizing the duration and geographic area of the interruption is critical.

When the decision to interrupt service is made, it must be communicated directly to public safety agencies and quasi-safety providers (such as alarm companies and emergency road service providers) by their respective wireless carriers as soon as possible. In the future, the alarm industry may eventually be able to develop strategies and technologies for mitigating the adverse impact of service interruptions to some degree, but only if alarm service providers are timely notified in advance of service interruptions. The same may be true of other safety-related industries and activities.

In conclusion, given the ever-increasing reliance the public safety community has upon wireless services and the likely-diminishing returns to be expected from intentionally interrupting those services, AICC believes the best solution is to avoid service interruptions to the greatest extent possible.

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Commission Seeks Comment on Certain Wireless Service Interruptions	)	GN Docket No. 12-52
	)	
	)	

To: The Commission

COMMENTS OF THE ALARM INDUSTRY COMMUNICATIONS COMMITTEE

The Alarm Industry Communications Committee ("AICC"), on behalf of its members[1] and pursuant to the Commission's Public Notice dated March 1, 2012,[2] hereby submits the following comments on several questions posed by the Commission regarding wireless service interruptions. For the Commission's convenience, AICC has reproduced and numbered below the questions to which it is responding, in the order presented in the Public Notice. In general, AICC believes that the aggregate harm of interrupting wireless service will almost always outweigh any potential benefit. The alarm industry heavily relies upon cellular devices to transmit alarm signals of all types, and citizens increasingly report emergencies to 911 via

[1] AICC is comprised of representatives of the Central Station Alarm Association (CSAA), Electronic Security Association (ESA), Bosch Security Systems, Digital Monitoring Products, Digital Security Control, Telular Corp, Stanley Convergent (alarm division, formerly known as Honeywell Monitoring), Honeywell Security, Vector Security, Inc., ADT Security Services, Inc., AES- IntelliNet, Alarm.com, Bay Alarm, Intertek Testing, RSI Videofied, Security Network of America, United Central Control, Security Industry Association (SIA), AFA Protective Systems, Vivint (formerly APX Alarm), COPS Monitoring, DGA Security, Security Networks, Universal Atlantic Systems, Axis Communications, Interlogix, LogicMark, Napco Security, Alarm Detection, ASG Security, Protection One, Security Networks, Select Security, Inovonics, Linear Corp., Numerex, Visonic, FM Approvals, and the Underwriters Laboratories.

[2] *Commission Seeks Comment on Certain Wireless Service Interruptions*, Public Notice, DA 12-311, GN Docket No. 12-311, released March 1, 2012.

wireless service. Silencing such transmissions, even for a limited time, would be extremely hazardous. At the same time, there is little evidence to show that disrupting service is effective; indeed, in some instances, it could make matters worse. At this time, AICC is not aware of a way to interrupt wireless service without also interrupting such wireless alarm signals and other emergency communications. Therefore, AICC respectfully submits that wireless service interruptions should be prohibited except under very narrow, well defined circumstances.

In particular, service interruptions should only be authorized where found by Federal authorities to be necessary to prevent imminent and significant loss of life, based on highly reliable intelligence confirmed by Federal intelligence resources, and upon a finding that there is a high probability the service interruption will prevent or significantly mitigate the threat. Any such interruption of service must be limited in duration and geographic scope to the shortest possible time, over the smallest possible area. To accommodate the possibility that intelligence may surface at the state or local level that may justify a service interruption, the Federal Government should set up a "hot line" procedure for vetting the perceived emergency through the above criteria on an expedited basis. Moreover, a procedure should be created to warn certain wireless-dependent safety activities that an interruption is taking place, so that they can attempt to mitigate the disruptive effects of this action. Each of these points is discussed herein:

2. Bases for interrupting wireless service. Under what circumstances, if any, is it appropriate for a public agency to interrupt wireless service? How effective is an interruption likely to be in achieving the purpose of the interruption?

AICC respectfully submits that the circumstances under which a wireless service interruption is appropriate are extremely limited, as a simple matter of cost outweighing benefit. The alarm industry alone uses approximately four million cellular devices as embedded wireless alarm relay radios in homes, businesses, schools, hospitals and government facilities, which

transmit signals alerting central stations about emergencies including fire, home invasions, carbon monoxide leaks and medical emergencies. Telematics vendors such as OnStar use commercial wireless networks to relay alerts when a driver has been in a serious accident. Victims of domestic violence use cell phones and cellular-based alarm devices to protect them from attacks. Furthermore, as the Commission has seen in its Next Generation 911 proceeding, wireless communications to 911 reporting a host of emergencies have grown by leaps and bounds.[3] Regardless of how likely it is that a wireless service interruption will achieve the desired outcome, it is unlikely the benefits associated therewith will outweigh the increased public safety risks due to the unavailability of wireless communications for other emergency communications that would otherwise take place during the period of the service interruption.

a. What types of government authorities are most likely to seek intentionally to interrupt wireless service?

Law enforcement entities of all levels could conceivably find a use for intentional service interruptions, and the BART incident[4] has shown that the pool of potential entities willing to employ interruptions is much larger. AICC recognizes that all of these state and local government entities, especially law enforcement, are staffed by dedicated employees who have taken it upon themselves to use any measure necessary to ensure the public's safety as part of their job; and these government agencies and their employees deserve the support of the Commission and industry in carrying out the important responsibilities they have undertaken. However, the use of wireless service interruptions as a government tool creates a ticklish issue,

[3] *See, e.g., Facilitating the Deployment of Text-to-911 and Other Next Generation 911 Applications; Framework for Next Generation 911 Applications*, Notice of Proposed Rulemaking, PS Dockets No. 11-153 and 10-225, released September 22, 2011, at ¶1 ("Sending text messages, photos, and video clips has become commonplace for users of mobile devices on 21st century broadband networks…").

[4] Press Release, BAY AREA RAPID TRANSIT, *Statement on temporary wireless service interruption in select BART stations on Aug. 11*, (Aug. 12, 2011), *available at* http://www.bart.gov/news/articles/2011/news20110812.aspx

much like the issue of cell phone jammers: Many government authorities wish to use jammers to block illegal cell phone use in prisons (a vexing problem crying out for a solution). However, other law enforcement authorities have gone on record as opposing the use of cell phone jammers in prisons, because they can block legitimate 911 calls outside the prison walls; and even prison guards have expressed concern that they will not be able to use their cell phones to call for help in the event of a threat to their safety inside the prison.[5] It is respectfully submitted that making wireless service interruptions available to all government entities, without some prioritizing oversight, will create a similar conflict.

A wireless interruption may accomplish the goal of one agency, while at the same time confounding the efforts of several other agencies. Once one government agency is permitted to effect a wireless service interruption, there is a high risk of creating a 'slippery slope' whereby it will be hard to tell other government agencies that they cannot use the same measure. As a result, potentially any government authority may be expected to seek access to wireless service interruption; yet very few agencies will have the overview and access to all relevant information necessary to know whether their use of a service interruption will confound the efforts of other agencies. Despite best efforts of dedicated public safety officials, their reaction to intelligence about an attack of some sort may have disastrous consequences. The news has been filled with instances where would be terrorists have been identified and caught in the act of a crime (thereby resulting in their incarceration) because the Federal intelligence community was able to set up a sting.[6] If State or local public safety officials somehow catch wind of the planned terrorist act

[5] *See, e.g.*, Matthew Harwood, *Hearing Weighs Pros and Cons of Phone Jamming Inside Prison*, Security Management, published July 15, 2009, available at http://www.securitymanagement.com/news/hearing-weighs-pros-and-cons-cell-phone-jamming-inside-prisons-005891; Public Knowledge, *Jamming Prison Cell Phones Threatens Public Safety, Groups Tell Senate*, published July 14, 2009, available at http://www.publicknowledge.org/node/2541l.

[6] For example, the attempted Times Square truck bombing (*see*, Murray Weiss, *Bomb suspect busted at JFK*, The New York Post, May 4, 2010, available at

without knowing that it is a sting, their use of a wireless service interruption may foil the Federal effort.

b. In what kinds of situations would a government authority potentially seek intentionally to interrupt wireless service? How frequently do these situations arise? For how long would service be interrupted in these situations? How rapidly after the threat to public safety has passed can service be restored?

AICC's concern about a 'slippery slope' extends to the determination of which situations warrant the use of a service interruption, as well. Reasonable people will disagree on the appropriateness of intentionally interrupting wireless service, meaning the situations in which a government authority would seek to do so will be varied and to some extent unpredictable. For example, BART stated it shut down service on August 11, 2011 because, "[a] civil disturbance during commute times at busy downtown San Francisco stations could lead to platform overcrowding and unsafe conditions for BART customers, employees and demonstrators."[7] Some agreed with BART's use of service interruption, while others found it a gross over-reaching of governmental authority.[8] While BART's concern was no doubt legitimate, it is not at all clear that the risk of platform overcrowding warranted an interruption that may have blocked a legitimate 911 calls or other such emergency communications that could have happened during the blackout. It is likely that other government agencies at all levels will look to the BART incident as a starting point in justifying the decision to interrupt service. Therefore, AICC believes the better course is to either ban wireless service interruptions entirely, or at minimum restrict such measure to a coordinated response to be taken only at the highest levels of the

---

http://www.nypost.com/p/news/local/bomb_suspect_busted_at_jfk_YcdVR3kBSvjTciTXytWRKI) , and more recently the attempted bombing of a military recruiting office in Catonsville, Maryland (*see* Tricia Bishop, *Would-be Catonsville bomber sentenced to 25 years in prison*, Baltimore Sun, April 6, 2012, available at *http://articles.baltimoresun.com/2012-04-06/news/bs-md-martinez-sentenced-20120406_1_muhammad-hussain-holy-war-vehicle-bomb).*

[7] Statement on temporary wireless service interruption in select BART stations on Aug. 11, *supra* fn. 4.

[8] Zack Whittaker, *San Francisco subway shuts off cell service to combat protest: Civil rights groups furious*, August 12, 2011, available at http://www.zdnet.com/blog/btl/san-francisco-subway-shuts-off-cell-service-to-combat-protest-civil-rights-groups-furious/54908.

Federal government. And regardless of the types or frequency of situations that may benefit from a service interruption, due to the widespread use of wireless service by the public for safety reasons, any interruptions must be as brief and limited as possible, and service must be restored as soon as possible.

c. Under what circumstances would an interruption of wireless service likely be effective in protecting public safety? Under what circumstances might interrupting wireless service be ineffective?

As an initial matter, AICC notes that any determination of 'effectiveness' must take into account the negative effect any individual measure has on other safety measures in use or in place. AICC believes that in the overwhelming majority of cases, wireless service interruption will likely do more harm than good. Even in a vacuum, however, interruptions of wireless service will likely only be effective in the event of a large-scale terrorist-style attack and, even then, only when based on extremely reliable, timely and specific intelligence. Unfortunately, even where such intelligence is available, interruption of wireless service is likely to be effective only the first few times, because the perpetrators will adapt by utilizing alternative methods. For example, the Public Notice refers to a hypothetical situation in which a cellular device may be used to detonate a bomb.[9] Effecting a wireless service interruption may prevent detonation the first time, but any time thereafter detonation could be accomplished another way, such as an unlicensed wireless device. In such a scenario, a government authority may have no way of knowing whether a bomb has a cellular detonator, and would be forced to interrupt service <u>just in case</u>. If the perpetrators in fact detonate the device by other means, the wireless service interruption will actually prevent the victims of the blast from calling for help, thereby compounding the damage done by the attack.

[9] Public Notice at p 1.

Moreover, if terrorists learn that they can cause government officials to order a shut down of public wireless services merely by threatening some sort of attack using wireless phones, they can make repeated false threats in order to cause maximum disruption of American life. Indeed, it is not inconceivable that terrorists and criminal elements could use the threat of an attack as a calculated method to temporarily knock out commercial wireless services, thereby disabling many wireless alarm devices and the public's means of reporting criminal activity.

As mentioned earlier, in circumstances other than terrorist attacks, the harms associated with interruptions of wireless service would likely far outweigh the benefits, if any. For example, in the case of flash mob crime, monitoring flash communications for intelligence that can be used to direct a law enforcement response, and then using the communications as evidence in later prosecutions, would likely prove the better alternative. The BART incident has already drawn considerable ire in the public forum, including comparisons to the totalitarian governments in North Africa and the Middle East that had blocked service in an attempt to disrupt protests there.[10] Any future use of wireless disruption in a protest situation could have the perverse effect of exacerbating the situation, incensing otherwise peaceful protesters. Such action can also embroil the government agency in litigation over alleged First Amendment violations. Indeed, legislation has already been introduced in California to block a repeat of the BART incident.[11]

[10] Wyatt Buchanan, *Bill Bars Cell Service Shutdown by Public Agencies*, San Francisco Chronicle, April 19, 2012, available at http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2012/04/18/MNQM1O5B1R.DTL#ixzz1syITMJG9 (last visited April 24, 2012).
[11] *Id.*

3. Risks in interrupting wireless service. What are the risks of an interruption of wireless service? What factors affect those risks?

As mentioned above, any interruption of wireless service carries with it a significant risk to public safety due to the increasing role that commercial wireless service plays in emergency communications. The Commission need look no further than its own NG911 proceeding, and the various steps it has taken to ensure redundant and quickly restorable wireless service,[12] to identify the potential pitfalls of intentionally disabling the service.

a. What public safety risks arise from intentionally interrupting wireless service? How are the activities of first responders and other emergency personnel and government authorities affected by an intentional interruption of wireless service? How are the activities of consumers affected by an intentional interruption of wireless service?

Wireless service interruptions create significant public safety risks: At any given time in a major city or suburb, numerous citizens are contacting 911 with medical emergencies that require immediate attention, or reporting crimes in progress, or automobile accidents that require an immediate response.[13] Often, prison guards and other public safety officials use wireless phones to communicate. Moreover, numerous private sector entities provide important services that save lives, thereby enhancing public safety while reducing the burden on state and local government entities.

For instance, as the Commission was advised during the analog cellular sunset proceeding, the alarm industry uses cellular devices as embedded wireless alarm relay radios in

[12] *See, e.g., Reliability and Continuity of Communications Networks*, Notice of Inquiry, PS Docket No. 11-60, released April 7, 2011; *In the Matter of Recommendations of the Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks*, Order, 22 FCC Rcd. 10541 (2007); 47 C.F.R. §§ 12.2, et seq. (2007) ("Redundancy of Communications Systems").

[13] As the Commission itself noted in the Public Notice, 70% of 911 calls currently come from wireless devices.

homes, businesses, schools, hospitals and government facilities;[14] the alarm industry estimates four million such devices are in use today. These devices transmit signals alerting central stations about emergencies including fire, home invasions, carbon monoxide leaks and medical emergencies. The central stations can then alert the appropriate authorities or, when appropriate, dispatch armed guards or implement other responses that allow public safety to better focus their scarce resources.

Use of wireless monitoring links as an alternative signaling path has become widespread, because a burglar or arsonist will often attempt to disable the transmission of alarm signals to the Central Station by cutting the telephone lines ordinarily used to transmit these signals. The alarm industry encounters thousands of line cuts each year, and this number is increasing.[15] Moreover, wireless alarm devices allow fire, medical and carbon monoxide alarm signals to reach the central station even if fire, storms, snow, fallen trees or other frequently occurring problems have damaged the telephone connection. When telephone service is disrupted, the wireless alarm device is the only way to send the necessary alarm signal. Loss of traditional wireline telephone service may be widespread during a terrorist attack.

[14] As of January 2007, the alarm industry had deployed approximately one million cellular service-based wireless alarm devices. See January 19, 2007 AICC Comments in RM-11355 at p. 23; February 6, 2007 AICC Reply Comments in RM 11355 at p. 31. The number of such devices deployed has grown substantially since 2007.

[15] *See* Jan. 19, 2007 AICC Comments pp. 3-6. Based on a 2001 study of this issue, the Security Industry Association (SIA) has concluded that line-cuts are increasing in frequency; line-cut is happening in homes almost as often as businesses; and it is being done by young amateurs (not just professional thieves). *See also, e.g.*, Dorchester Reporter, "Recent Break-in Pattern Targets Local Pubs", January 27, 2005 ("The burglars cut phone lines, disabling the alarm system, and broke the back door lock . . ."); Victorville Daily Press, "California Book Theft Ring Broken", February 17, 2006 ("The M.O. was to cut the phone lines to disable the alarm systems and then they would take the security tapes before they left."); Longford Today, "Thieves Target Home of Prominent Publican", January 3, 2007 ("The cutting of the phone lines disabled Kevin's burglar alarm, allowing the culprits to access the premises . . ."); Cellular alarm radios not only serve as the secondary link to the central station, but also often have the ability to signal the alarm company when a line cut occurs. This can place the alarm company in the position of contacting the customer or local authorities before the break-in has been accomplished.

Wireless alarm devices are not just used to protect homes and businesses. Many of the premises protected by such devices are vital to public safety:

Governmental Facilities
Airports
Department of Defense facilities
Department of Homeland Security facilities
U.S. Marshals Service facilities
Federal courthouses
State Highway Administration
State Government Offices
Federal Government Offices supporting National security efforts of Department of Energy, Central Intelligence Agency, and National Security Agency
Municipal Utilities
County water treatment plants
Public dams
Public port facilities
Public libraries
Municipal museums

Critical Infrastructure Facilities
Hospitals
Domestic abuse shelters
Power plants
Pharmaceutical plants
Chemical plants
Banks and credit unions
State and private educational institutions

Cellular-based wireless alarm systems are also used to protect victims of domestic abuse, with certain programs providing abuse victims with free cell phones or cellular-based alarm devices that can be used to summon help in the event of an attack.[16] In addition, cellular

[16] The ADT AWARE® program exemplifies how security systems can be used by victims of domestic violence. AWARE systems are provided to a select group of victims within covered communities. All have reported domestic violence and have agreed to prosecute their abusers. The cellular component minimizes the impact of an abuser cutting the phone line. Systems include a panic button that sends a priority emergency signal with a single button press. 170 communities have adopted AWARE and the program is credited with saving the lives of at least 34 people. Beyond the AWARE program, many victims of violence rely upon monitored security systems. 1 in 4 women will experience domestic violence in their lifetime (National Center for Victims of Crime, www.ncvc.org). Intimate Partner Violence results in nearly 2 million injuries and 1,300 deaths nationwide every year (CDC 2003).

communications are used extensively for Enhanced Alarm Verification to verify emergency situations, reduce false alarms and reduce the unnecessary deployment of valuable life safety resources. In certain states, all central stations that handle residential or commercial intrusion/burglary alarm activations are required to make at least two phone calls in an attempt to verify the validity of any monitored alarm activation. Alarm companies are finding that dialing a customer's cell phone is one of the most effective ways to quickly verify whether authorities need to be dispatched.

Other private sector uses of wireless service to save lives and improve public safety include, e.g., OnStar and other emergency road services. Because of these vital safety-related activities that depend on the commercial wireless networks, the FCC has wisely prohibited the use of cell-phone jammers. For the same reasons, the Commission must not allow frequent interruptions to wireless service by government agencies.

As time marches on and industry and technology progress, the risks are bound only to increase. For example, an increasing number of wireless systems monitored by the alarm industry use cellular networks as the sole communications path to the central station. While this was predominantly the case for residential alarm systems in the past, the changes introduced in the 2010 edition of National Fire Alarm and Signaling Code (NFPA) also allowed cellular as the sole communication path for commercial fire systems. Shutting down the sole path of communication for these systems could result in increased property damage and loss of life due to delayed response from emergency services. Likewise, wireless communications play a growing role, as seen in the roll-out of NG911, a primary thrust of which is to increase the ability for citizens to use wireless communication, such as text and multimedia messaging, when contacting 911.

b. What are the potential economic consequences of intentionally interrupting wireless service?

Repeated wireless service interruptions can stop a significant amount of commerce, and more importantly undermine the public's confidence in wireless services. Our society is in the midst of a revolution whereby most transactions can now be conducted using wireless devices, including everything from buying a coffee to paying at a parking meter. While this economic impact can be significant, AICC is more focused on the threat to the lives and property of families and businesses using wireless alarm devices.

c. How do particular circumstances affect the risks that arise from an interruption of wireless service? Are there particular kinds of locations where interruption is especially risky? Are there areas where first responders and other emergency personnel are especially dependent upon commercial wireless service to perform their duties or where consumers are particularly dependent on wireless service? How does the availability of alternative means of communication affect the risks that arise from an interruption of wireless service? Does the interruption of wireless service pose particular risks to persons with disabilities?

The dependence of the public and industry on commercial wireless services is growing exponentially. While the internet offers alternative channels of communication, persons need a means to send internet traffic. Many depend on wireless services not only for mobile communications but as their sole access to the Internet and the Public Switched Telephone Network. Preliminary results from the January–June 2011 National Health Interview Survey (NHIS) indicate that the number of American homes with only wireless telephones continues to grow.[17] More than 3 of every 10 American homes (31.6%) had only wireless telephones (also known as cellular telephones, cell phones, or mobile phones) during the first half of 2011—an

[17] Stephen J. Blumberg, Ph.D., and Julian V. Luke, *Wireless Substitution: Early Release Estimates from the National Health Interview Survey, January – June 2011*, Department of Health Interview Statistics.

increase of 1.9 percentage points since the second half of 2010.[18] In addition, nearly one of every six American homes (16.4%) received all or almost all calls on wireless telephones despite also having a landline telephone.[19] Because the use of wireless alarm devices is widespread, especially in urban and suburban areas, it is difficult for AICC to say that there are areas where it is "safe" to interrupt wireless service. In addition, millions of seniors and persons with disabilities utilize "panic button" stationary Personal Emergency Response Systems (PERS) and mobile (MPERS) devices that rely not only on an unlicensed device to link them to the alarm panel, but commercial wireless service to relay the panic message to the central station so that help can be summoned. In May 2011, the first of 77 million U.S. baby boomers turned 65 years of age,[20] adding to the user population for PERS. PERS enhances the safety net for these people to secure help in emergency situations and allow the users to remain independent versus moving to a care facility.

d. What steps could be taken to minimize the risks that arise from an interruption of wireless service? What steps could be taken to narrow the scope of a service interruption?

First, wireless service interruptions should not be permitted without some proof of the necessity of such an act. Along these lines, State Sen. Alex Padilla, D-Pacoima (Los Angeles County) proposed a state bill in California in response to the BART incident which requires an order signed by a judicial officer that includes all of the following findings: (1) That probable cause exists that the service is being or will be used for an unlawful purpose or to assist in a violation of the law; (2) That absent immediate and summary action to interrupt communications service, significant danger to the public health, safety, or welfare will result; and (3) That

[18] *Id.* at p 2.
[19] *Id.* at p 4.
[20] Frederica D. Kramer and Demetra Smith Nightingale, Aging Baby Boomers In a New Workforce Development System, U.S. Employment and Training Administration, 2001.

interruption of communications service will not suppress speech that is protected by the First Amendment to the United States Constitution or Section 2 of Article I of the California Constitution, or violate any other rights under federal or state law.[21] AICC agrees with the spirit of Senator Padilla's proposed legislation, but believes an even more restrictive protocol should be adopted (as discussed below), in the event intentional service interruptions are permitted.

Second, to the extent that any situation can be found to justify a service interruption, minimizing the duration and geographic area of the interruption is critical. AICC has consulted with manufacturers of wireless alarm devices, such as Telular, Inc., to determine whether it would be possible to suppress just the voice channels of a wireless service while leaving data/control channels operational, as a way to allow alarm devices to continue working. Unfortunately, AICC has been advised that this would not be effective. In looking to see if there was a work-around or if certain channels/services could still operate if a government agency interrupted services, alarm manufacturers found that any alarm traffic sent via a cellular control channel, or over GPRS, 3G or 4G data channels, would be impacted. Moreover, criminal elements would likely switch their tactics to use whatever communications channel is left operational. AICC does not rule out the possibility that the wireless industry could develop a technical solution to this issue, just as alternatives to cell phone jamming are being deployed for use in prisons.[22] However, it does not appear that an effective technical solution exists at this time.

[21] SB 1160 (Ca. 2012).
[22] *See, e.g.*, Lynnette Luna, Tecore Offers Alternative to Cell-Phone Jamming Equipment, Urgent Communications, published February 11, 2009, available at http://urgentcomm.com/policy_and_law/news/tecore-cell-jamming-alternative-0211/.

e. What institutions or officials should be notified of an intentional interruption of wireless service? How and when should they be notified? How and when should the public be notified? Should notifications include the reason for the service interruption?

It is imperative that a decision to interrupt service be communicated directly to public safety agencies and quasi-safety providers (such as alarm companies and emergency road service providers) as soon as possible by their respective wireless carriers, rather than in reliance on a method involving several levels of retransmission. This communication method must outline all the possible services impacted beyond regular cell phone use, including property and life-safety monitoring equipment such as PERS systems, home security alarms, and commercial fire monitoring, etc. Wireless carriers should ensure safety-related operations are aware of the approximate time and location of the service interruption – perhaps "fudged" just a bit (as has been done for GPS data) in case the warning becomes public.

The alarm industry may eventually be able to develop strategies and technologies for mitigating the adverse impact of service interruptions to some degree, if alarm service providers are timely notified in advance of service interruptions. The same may be true of other safety-related industries and activities. However, AICC believes the best solution is to avoid service interruptions to the greatest extent possible.

Finally, AICC notes that wireless carriers should also provide language that could be inserted in all agreements with end user customers to ensure they are aware of and acknowledge the ability of the government to request an interruption of cellular service as deemed necessary.

f. Are there less intrusive ways of protecting public safety than interrupting wireless service? If so, what are they? Under what circumstances are these alternative means likely to be as effective as interrupting wireless service? Should government officials be required to consider alternative means before interrupting wireless service?

As discussed above, it will be necessary to develop alternative ways of dealing with criminal activities because, after the first few publicized instances of attacks being averted by a service interruption, bad actors will change strategies. Even now, it is likely that the BART incident will be in the minds of future terrorists and would-be criminals.

g. Are there situations where the risk of interrupting wireless service will always outweigh the benefits?

In the absence of reliable information about the exact time, location and means of an attack with potential widespread consequences (mass casualties), the risk of a service interruption will almost always outweigh the benefit: Genuine emergencies (heart attacks, home invasions, fires, auto accidents) will go unreported to public safety and/or central stations, and authorities will never know when the expected service interruption is actually a part of the criminals' strategy.

5. Authority to interrupt service.

Any service interruption must be made by Federal officials with access to specific threat information from reliable Federal intelligence resources. While these officials could assess locally-developed intelligence and work with state and local officials as appropriate, the decision to actually interrupt service should be made at the highest level of the Federal intelligence community. As discussed above, in order to accommodate state and local concerns and intelligence sources, a "hot line" procedure should be developed. But in general, it is only the

Federal intelligence community (NSA, CIA, Military intelligence departments), under existing Federal oversight, that appear to have the capabilities to verify threat information and formulate a coordinated response that will not create more harm than good. And even in the hands of the Federal intelligence community, strict protocols must be developed to limit the use of service interruptions.

Conclusion

In conclusion, the benefits of wireless service interruption appear greatly outweighed by the risks in most circumstances. The possibility of interrupting emergency communications along with other traffic is simply too great. Therefore, the Commission should not permit wireless service interruption at this time, except under the very limited circumstances and under the strict protocols discussed above.

Respectfully submitted,

Alarm Industry Communications Committee

By: s/ John A. Prendergast

John A. Prendergast
Salvatore Taillefer, Jr.

Its Attorneys

Blooston, Mordkofsky, Dickens,
Duffy, & Prendergast, LLP
2120 L Street NW
Suite 300
Washington DC 20037
Tel: 202-659-0830

Filed: April 30, 2012